PATTON BOGGS LLP
ATTORNEYS AT LAW

1660 Lincoln Street, Suite 2050
Denver CO 80264
(303) 830-1776

Facsimile: (303) 894-9239

FAX TRANSMISSION

DATE:	August 22, 2006
PTO IDENTIFIER:	**Application Number** 10/028,004-Conf. #2388 **Patent Number**
Inventor:	Robert R. Gilman et al.
MESSAGE TO:	MS Appeal Brief – Patents (USPTO)
FAX NUMBER:	(571) 273-8300
FROM:	PATTON BOGGS LLP Carl A. Forest
PHONE:	303-894-6114
Attorney Dkt. #:	013217.0177PTUS (401043-A-01-US)
PAGES (Including Cover Sheet):	28
CONTENTS:	Certificate of Transmission (1 page) Appellants' Revised Appeal Brief (26 pages)

PATTON BOGGS LLP
1660 Lincoln Street, Suite 1900, Denver, Colorado 80264
Telephone: (303) 830-1776 **Facsimile:** (303) 894-9239

239529

RECEIVED
CENTRAL FAX CENTER

AUG 2 2 2006

PTO/SB/97 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U. S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Application No. (if known): 10/028,004

Attorney Docket No.: 013217.0177PTUS
(401043-A-01-US)

Certificate of Transmission under 37 CFR 1.8

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office.

on August 22, 2006
Date

Elaine C. VonSpreckelsen
Signature

Elaine C. VonSpreckelsen
Typed or printed name of person signing Certificate

N/A
Registration Number, if applicable

(303) 894-6163
Telephone Number

Note: Each paper must have its own certificate of transmission, or this certificate must identify each submitted paper.

Appellants' Revised Appeal Brief (26 pages)

RECEIVED
CENTRAL FAX CENTER

AUG 2 2 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
ON APPEAL BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Patent Application Serial No. 10/028004	Confirmation No.: 2388
Filing Date: December 21, 2001	Art Unit: 2134
For: Secure Data Authentication Apparatus	Examiner: T.M. Szymanski
Inventors: Robert R. Gilman, Richard L. Robinson, and Douglas A. Spencer	Docket No.: 013217.0177PTUS (401043-A-01-US)

MAIL STOP APPEAL BRIEF – PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Dear Sir:

APPELLANTS' REVISED APPEAL BRIEF

Appellants' Appeal Brief was timely filed pursuant to 37 CFR §1.192 because it was filed within two months of 28 March, 2006, which is the date on which Appellants filed their Notice of Appeal. This Revised Appeal Brief corrects a number of informalities noted in the Notification of Non-Compliant Brief dated 24 July 2006.

Appellants believe that the claims appealed are patentable as argued in the Appeal Brief. If the Examiner has any questions concerning the Appeal Brief or the Arguments presented in the Appeal Brief and feels that an interview pursuant to MPEP Sections 713.05 and 713.09 may be helpful in resolving the issues on appeal, attorneys for the Appellants would urge the Examiner to contact the attorneys for Appellants to arrange such an interview, even if the refiling of this application is necessary for this purpose.

Appellants' attorneys respectfully solicit the Board to remand this case to the Examiner with instructions to allow the case.

Application No. 10/028004
Appellant's Appeal Brief

Docket No.: 013217.0177PTUS
(401043-A-01-US)

Table of Contents:

List of References

U.S. Patent No. 5,724,425 issued to Chang et al.

U.S. Patent Publication No. 2002/0073325 issued to Ho.

U.S. Patent No. 6,044,469 issued to Horstmann.

OUTLINE OF APPEAL BRIEF

1.) REAL PARTY IN INTEREST

The party named in the caption of the Appeal Brief is Avaya Technology Corp.

A full list of inventors is: Robert R. Gilman, Richard L. Robinson, and Douglas A. Spencer.

The subject matter of the invention was derived from research efforts undertaken by Robert R. Gilman, Richard L. Robinson, and Douglas A. Spencer in Denver, Colorado.

The rights to the present invention were assigned by the inventors Robert R. Gilman, Richard L. Robinson, and Douglas A. Spencer in an Assignment document dated December 19, 2001 and filed on December 21, 2001, recorded at Reel 012412 and Frame 0172 on December 21, 2001.

The real party of interest is accordingly Avaya Technology Corp. because Avaya Technology Corp. owns the entire right, title, and interest to the present invention.

2.) RELATED APPEALS AND INTERFERENCES

Currently, no appeals or interferences are known by any party.

3.) STATUS OF THE CLAIMS

Claims 1 – 15 and 18 are pending. In a Final Office Action mailed 30 November 2005, the Examiner rejected claims 16 and 17 under 35 USC §102(b) as being anticipated by Chang et al. (US Patent No. 5,724,425). The Examiner also rejected claims 1 – 5, 10 – 14, 16, and 17 under 35 USC §103(a) as being unpatentable over Chang et al. (US Patent No. 5,724,425), and further in view of Ho et al. (US Patent Application Publication No. 2002/0073325), and claims 6 – 9, 15, and 18 under 35 USC §103(a) as being unpatentable over Chang et al. (US Patent No. 5,724,425), and Ho et

al. (US Patent Application Publication No. 2002/0073325), as applied to claim 1 above, and further in view of Horstmann (US Patent No. 6,044,469). Appellants filed an Amendment After Final on 15 Feb 2006, canceling claims 16 and 17 and addressing the Examiner's rejections of claims 1 – 15 and 18 that were based on the newly cited Ho U.S. Published Patent Application. The Examiner entered the Amendment and issued an Advisory Action on 28 Feb 2006, reasserting the above-noted rejections of claims 1 – 15 and 18.

4.) STATUS OF AMENDMENTS

Appellants filed an Amendment After Final on 15 Feb 2006, canceling claims 16 and 17 and addressing the Examiner's rejections of claims 1 – 15 and 18. The Examiner entered the Amendment and issued an Advisory Action on 28 Feb 2006, reasserting the rejections of claims 1 – 15 18 noted above.

5.) SUMMARY OF CLAIMED SUBJECT MATTER

The pending claims define a method for authenticating: 1.) the source of a software file, 2.) owner of the software file, and 3.) the telephony switching system on which the software file is being installed. The software file is hashed using a selected hash algorithm. The hash value is then encrypted with the unique owner key, which is assigned to the telephone system on which the software file is to be installed, to calculate an owner specific source signature. The benefit of creating a unique owner specific source signature to append to the installation software is to prevent unauthorized individuals, who may obtain the software file in an unscrambled form, from using the software file without authorization. Once calculated, the unique owner specific source signature is appended to the software file. A secure microprocessor is located within the telephony switching equipment and includes an encryption algorithm, a security routine, a source key, and the unique owner key that are used by the secure microprocessor to calculate a target telephony switching system signature for each software file or downloaded image. The secure microprocessor compares the calculated target telephony switching system signature to the owner specific source signature appended to the end of the software file or images. If the signatures match,

installation and use is authorized. If the signatures do not match, the software file cannot be installed and the telephony switching system may be disabled.

Independent Claim 1

1. (Previously presented) A secure data authentication apparatus 150 to authenticate a software file 300, the software file having a first signature 340 appended to the software file 300, for use on a computer system 100, wherein said computer system 100 is assigned an owner key 210 that is unique to said computer system 100, said first signature 340 comprising a source hash value 230 that is computed by processing at least some of said software file 300 using a selected hash function, which source hash value 230 is encrypted using said owner key 210 to produce said first signature 340, the apparatus comprising:

a secure processing device 150 within the computer system 100 to receive the software file 300 and hash the software file 300 using said selected hash function to produce a first hash value 240 (Page 14, Lines 11 – 19); and

a first key 272 located within the secure processing device 150, which first key 272 comprises said owner key 210 the secure processing device 150 encrypts the first hash value 240 with the first key 272 to generate a second signature 430 and compares the first signature 340 with the second signature 430, and if the first signature 340 matches the second signature 430, the computer system 100 accepts the software file 300 as being authenticated (Page 16, Line 3 – Page 17, Line 7).

Independent Claim 7

7. (Previously presented) A secure data authentication apparatus 150 to authenticate an owner of a software file 300 and of a telephony switching system 100 on which the software file 300 is stored, the apparatus comprising:

a first feature file 310 and a software file 300, the first feature file 310 having a plurality of features and a first owner signature 340 appended thereto, wherein said telephony switching system 100 is assigned a first owner key 210 that is unique to said telephony switching system 100, said first owner signature 340 comprising a source hash value 230 that is computed by processing at least some of said software file 300 using a selected hash function, which source hash value 230 is encrypted using said

first owner key 210 to produce said first owner signature 340, wherein a first subset of the plurality of features is activated (Page 13, Line 24 – Page 15, Line 7);

a secure microprocessor 150 within the telephony switching system 100, the secure microprocessor 150 having an encryption algorithm, wherein the secure microprocessor 150 hashes the first feature file 310 using said selected hash function to generate a first hash value 240 (Page 11, Line 23 – Page 12, Line 3; Page 14, Lines 11 – 21); and

a first owner key 210 within the secure microprocessor 150, wherein the secure microprocessor 150 encrypts the first hash value 240 with the first owner key 210 to generate a second owner signature 430 and the secure microprocessor 150 compares the first owner signature 340 with the second owner signature 430, and if the first owner signature 340 matches the second owner signature 430, the telephony switching system 100 operates in accordance with the first subset of the plurality of features of the first feature file 310 (Page 16, Line 3 – Page 17, Line 7).

Independent Claim 10

10. (Previously presented) A method for authenticating an owner of a software file 300 that has a first identification code comprising a source hash value 230 that is computed by processing at least some of said software file 300 using a selected hash function, which source hash value 230 is encrypted using an owner key 210 to produce said first signature 340, attached thereto for use on a computer system 100, wherein said computer system 100 is assigned said owner key 210 that is unique to said computer system 100, the computer system 100 comprising a secure processor 150 having an encryption algorithm and an owner key 210, the method comprising:

initiating the computer system 100 (Step 410, Page 16, lines 3 – 6);

hashing the software file 300 using said selected hash function within the secure processor 150 to generate a first hash value 230 (Step 420, Page 16, Lines 6 – 8);

encrypting the first hash value 230 with the owner key 210 to generate a second identification code 430 (Step 430, Page 16, Lines 8 – 10); and

comparing the first identification code 340 with the second identification code 430, and if the first identification code 340 matches the second identification code 430,

the computer system 100 accepts the software file 300 as being authenticated for the owner's use (Step 440, Page 17, Lines 1 – 7).

Independent Claim 11

11. (Previously presented) A method for authenticating an owner of a software file 300 that has a first owner signature 340 comprising a source hash value 230 that is computed by processing at least some of said software file 300 using a selected hash function, which source hash value 230 is encrypted using an owner key 210 to produce said first signature 340, appended to the software file 300, for use on a computer system 100, wherein said computer system 100 is assigned said owner key 210 that is unique to said computer system 100, having a secure processing device 150 to generate an authorization signal, the secure processing device 150 comprising a security routine, an encryption algorithm and a first owner key, the process comprising:

receiving the software file 300 by the computer system 100 and sending the software file 300 to the secure processing device 150 (Step 410, Page 16, Lines 3 – 6);

hashing the software file 300 using said selected hash function to generate a first hash value 240 (Step 420, Page 16, Lines 6 – 8);

encrypting the first hash value 240 within the secure processing device 150 with the first owner key 210 to generate a second owner signature 430 (Step 430, Page 16, Lines 8 – 10); and

comparing the first owner signature 340 to the second owner signature 430, wherein if the first owner signature 340 and the second owner signature 430 match, the secure processing device 150 generates the authorization signal (Step 440, Page 17, Lines 1 – 7).

Independent Claim 18

18. (Previously presented) A method for authenticating a software file 300 from a PBX manufacturer, the software file 300 comprising a feature file 310 having a plurality of features wherein a subset of the plurality of features are activated, the software file 300 operating on a PBX 100, the PBX 100 comprising a secure microprocessor 150 having an encryption algorithm and a first key 210 that is unique to said PBX 100, the method comprising:

hashing the feature file 310 using a selected hash function at the PBX manufacturer to generate a first hash value 230 (Step 230, Page 14, Lines 11 and 12);

encrypting the first hash value 230 with said first key 210 to generate a first signature 340 (Step 240, Page 14, Lines 12 – 19);

appending the first signature 340 to the feature file 310 (Step 250, Page 14, Lines 19 – 21);

receiving the feature file 310 and appended first signature 340 by the secure microprocessor 150 (Step 410, Page 16, lines 3 – 6);

hashing the received feature file 310 using said selected hash function within the secure microprocessor 150 to generate a second hash value 420 (Step 420, Page 16, Lines 6 – 8);

encrypting the second hash value 420 with the first key 210 to generate a second signature 430 (Step 430, Page 16, Lines 8 – 10); and

comparing the first signature 340 with the second signature 430, and if the first signature 340 matches the second signature 430, the PBX 100 accepts the software file 310 as being authenticated (Step 440, Page 17, Lines 1 – 7).

6.) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues on appeal are whether the final rejection of rejected claims 1 – 5, 10 – 14, 16, and 17 under 35 USC §103(a) as being unpatentable over Chang et al. (US Patent No. 5,724,425), and further in view of Ho et al. (US Patent Application Publication No. 2002/0073325), and claims 6 – 9, 15, and 18 under 35 USC §103(a) as being unpatentable over Chang et al. (US Patent No. 5,724,425), and Ho et al. (US Patent Application Publication No. 2002/0073325), as applied to claim 1 above, and further in view of Horstmann (US Patent No. 6,044,469) should be reversed.

Appellants submit that the 35 U.S.C. §103(a) rejection of claims 1 – 15 and 18 set forth in the Final Office Action dated 30 November 2005 fails to set forth a prima facie showing of obviousness because:

(1) the Examiner has failed to cite and apply references which contain all of the claimed elements or limitations of Appellants' claimed invention, and

(2) the Examiner has not shown where the prior art, the nature of the problem to be solved, or the knowledge of those skilled in the art provide any motivation

or suggestion to combine elements in the prior art relied upon by the Examiner to render the claimed invention obvious, and instead has relied upon hindsight to reconstruct Appellants' claimed invention from the prior art.

Appellants submit that the Examiner has failed to address any of Appellants' arguments presented in the Amendment After Final dated 15 February 2006 or present any reasoning why he believes the specific claim language identified by Appellants in this response is shown by either the cited Chang Patent or the cited Ho Published Patent Application.

7.) ARGUMENT

I. Examiner's Position – Rejection under 35 U.S.C. §103(a)

The Examiner rejected claims 6 – 9, 15, and 18 under 35 USC §103(a) as being unpatentable over Chang et al. (US Patent No. 5,724,425), and Ho et al. (US Patent Application Publication No. 2002/0073325), as applied to claim 1 above, and further in view of Horstmann (US Patent No. 6,044,469). The Examiner noted with respect thereto:

> Chang et al ("Chang") has taught the method of authentication as in the claimed invention, but fails to teach the implementation of an owner key that is unique to the given computer system.
>
> Ho et al. ("Ho"), however, teaches the use of a key specific to the individual computer system for the purposes of license integrity.
>
> It is desirable to maintain the authenticity of a software program from malicious attack by worms, viruses, and other programs or individuals that have the common intent of harming a host system. Such programs are known to often compromise critical information of such a system and cause additional damage. As taught by Chang, such attacks are avoidable by the implementation of a signature system that is composed of a message digest to confirm the integrity of the software. Ho teaches that a greater level of security may be obtained by the implementation of a unique key signature of a system so as to prevent that particular license from being compromised (Ho paragraphs 4 – 12, Chang, Col. 1 line 50 – Col. 3 line 13).

II. Appellants' Characterization of the References

The cited Chang Patent teaches that, to protect a source code file, a software application writer's private key, along with an application writer's license, is provided to a first computer. The application writer's license includes identifying information, such as the application writer's name, as well as the application writer's public key. A compiler program executed by the first computer compiles the source code into binary code and computes a message digest for the binary code. The first computer then encrypts the message digest using the application writer's private key, such that the encrypted message digest is defined as a digital "signature" of the application writer. A software passport is then generated which includes the application writer's digital signature, the application writer's license, and the binary code. A user, upon receipt of the software passport, loads the passport into a computer, and the user's computer computes a second message digest for the software passport and compares it to the first message digest, such that if the first and second message digests are not equal, the software passport is also rejected by the user's computer and the code is not executed.

However, as noted by the Examiner, "Chang ... fails to teach the implementation of an owner key that is unique to the given computer system," which structure is affirmatively recited in Applicants' independent claims.

The Examiner relies on the cited Ho Patent that teaches:

> A method and an apparatus for using an encrypted unique digital signature ("engraved signature") as a uniquely definable signature to control the use or execution of software in a computer system. The computer system has a Network Interface Card ("NIC") with a Media Access Control ("MAC") address. On start up, the engraved signature is retrieved from the persistent storage medium of the computer system and the MAC address is retrieved from the NIC. A computed encrypted signature is generated using the MAC address. Where the computed encrypted signature does not match the engraved signature, the execution of the software is halted. (Abstract)

However, the Ho Patent is limited to a self-contained storage medium and a network interface card, as noted in paragraphs [0008] – [0010]:

> [0008] The problem of software piracy is acute with a particular class of computer systems: Internet Appliances. An Internet Appliance is generally a computer system that performs some predetermined functions while connected to the Internet. The Internet Appliances typically consist of computer hardware with embedded software. The hardware includes a storage medium and a network interface card.
>
> [0009] Software embedded in an Internet Appliance tends to be compact. It is not uncommon to store the entire system software in a storage medium that has only a few megabytes of capacity. This type of storage medium is usually small and very portable (such as CompactFlash and SIM cards). Because of wide adaptation and portability of such media, digital content inside such mediums can be illegally duplicated very easily.
>
> [0010] It is therefore an aspect of an object of the present invention to provide a method and an apparatus for protecting the embedded software in computer systems, such as Internet Appliances, against unauthorized use, while being relatively cost-effective to deploy.

The Ho Patent further notes that it is impractical to execute a unique compilation of the software for each end user computer:

> [0005] Restricted entitlement means that the software contains some means to limit itself to run only on the computer system for which it is authorized. A common restriction method is to encode hardware specific information in the computer system so that the software can verify the information at system startup. Another method is to make the software unique for every computer system. This entails unique compilation of the software for each distribution, which is a very costly operation.

Therefore, the Ho Patent specifically rejects the combination noted by the Examiner (and claimed by Appellants), since the use of a computer-specific encoding is impractical. Instead, the Ho Patent relies on the fact that the target type of software is an Internet Appliance where "The Internet Appliances typically consist of computer hardware with embedded software. The hardware includes a storage medium and a network interface card." Thus, the Ho Patent relies on the software to be distributed as

part of the hardware of the Internet Appliance and does not envision transmission of programs over a network to the end user computer.

The Horstmann Patent discloses a software protection mechanism that may be conveniently configured by a software publisher and applied to a software product. Various predefined software protection measures are presented to the software publisher, who selects which protection measures, if any, the software publisher wishes to apply to a software product. The software publisher's selections are saved in a license file that is attached to the software product. A Protector Module is also attached to the software product. The Protector Module includes code for each predefined software protection option. When an attempt is made to run the software product, the Protector Module reads the license file and executes code for each software protection option that has been selected. The resulting software protection mechanism provides the software publisher complete control over the trade-off between security and user convenience.

III. Appellants' Position

Appellants disagree with the Examiner's 35 U.S.C. §103(a) rejection of claims 1 – 15 and 18 as being unpatentable because the Examiner failed to establish a prima facie case of obviousness of Appellants' claimed invention for the following two reasons:

A. The Examiner has failed to cite and apply prior art which contain all of the claimed elements or limitations of Appellants' claimed invention; and

B. The Examiner has failed to identify any motivation or suggestion to combine elements from the prior art to render the claimed invention obvious, and instead has relied upon hindsight to reconstruct Appellants' claimed invention from the prior art.

The Examiner has presented a multitude of references, each directed to a different class of system in the field of data file encryption, all of which teach away from each other and away from Appellants' claimed system. The Examiner has excerpted isolated fragments of these references, which are used to draw an analogy to various individual elements recited in Appellants' claims, without an associated linking of the relevance of the overall system to show motivation or suggestion to combine, since these disparate

systems are not consistent in form or purpose among themselves or with Appellants' method for authenticating the source of a software file as well as the owner of the software file and the telephony switching system on which the software file is being installed. However, when the excerpts from the references are analyzed in the proper context, they fail to show or suggest the corresponding structure in Appellants' claims.

In contrast to the teachings of the cited references, Appellants' secure data authentication apparatus makes use of a file transmission protocol where "the software file having a first signature appended to the software file", and the user's "computer system is assigned an owner key that is unique to said computer system." The hash value is computed "by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said owner key to produce said first signature." Furthermore, Appellants' secure data authentication apparatus includes "a first key located within the secure processing device, which first key comprises said owner key wherein the secure processing device encrypts the first hash value with the first key to generate a second signature." When the user's computer receives the software file and the associated digital signature, it can recompute the digital signature using an owner's key that is specific to the target telephone switching system and compare it to the received digital signature. Thus, Appellants' independent claim 1 recites structure that is not shown or suggested by the cited references, since the Ho Patent specifically teaches away from the combination suggested by the Examiner.

IV. Discussion of Lack of Prima Facie Obviousness

The courts and the MPEP state that to reject a claim for obviousness under 35 U.S.C. 103(a), the Examiner must make a prima facie showing of obviousness before the burden shifts to the Appellant to prove non-obviousness.

Appellants believe that the Examiner has not made a prima facie showing of obviousness for the claimed invention under 35 U.S.C. 103(a). The prior art relied upon by the Examiner must disclose all of the claim elements or limitations in order to make a prima facie showing of obviousness. Also, the MPEP and courts have stated that the Examiner must show the following:

> 1.) A motivation or suggestion to combine references; 2.) A reasonable expectation of success from combining the references; and 3.) The

combined references teach all of the limitations of the claimed invention. MPEP 706.02(j); See also *In re Vaeck*, 20 USPQ2d 1438 (Fed. Cir. 1991).

If any of these requirements are not met, the combination of the references does not establish a prima facie showing of obviousness for the claimed invention. The Examiner has not met any of the requirements of this test.

V. Comparison of the Claims with the Prior Art Illustrating the Failure of the Prior Art to Disclose Key Claimed Elements or Limitations

The independent claims are claims 1, 7, 10, and 11. Claim 1 is the broadest independent claim and is illustrative of claims 1 – 15 and 18 for the purposes of this discussion. The following analysis of the claims is summarized in claim chart form with regard to the independent claim 1, since independent claims 7, 10, and 11 are analogous in scope. All of the remaining claims depend on independent claims 1, 7, 10, or 11 and, therefore, are distinguishable over the prior art in the same manner as the independent claims and specifically independent claim 1.

VI. Claim Chart

The following claim chart compares Appellants' claim 1 with the cited Chang Patent and the Ho Patent Application Publication that were noted above and relied upon by the Examiner in the rejection of claim 1, with the elements of Appellant's claim 1 not shown in the cited Chang Patent and the Ho Patent Application Publication being underlined. The failure of these references to teach all of the elements recited in claim 1 (and analogous limitations in independent claims 7, 10, and 11) supports Appellants' position that the Examiner has failed to make a prima facie showing of obviousness under 35 U.S.C. 103(a), thereby rendering claims 1 – 15 and 18 allowable.

Appellants' Claim 1	Chang Patent	Ho Published Patent Application
A secure data authentication apparatus to authenticate a software file, the software file having a first signature appended to the software file, for use on a computer system, wherein said computer system is assigned an owner key that is unique to said computer system, said first signature comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said owner key to produce said first signature, the apparatus comprising: a secure processing device within the computer system to receive the software file and hash the software file using said selected hash function to produce a first hash value; and a first key located within the secure processing device, which first key comprises said owner key wherein the secure processing device encrypts the first hash value with the first key to generate a second signature and compares the first signature with the second signature, and if the first signature matches the second signature, the computer system accepts the software file as being authenticated.	The Chang Patent teaches that, to protect a source code file, a software application writer's private key, along with an application writer's license, is provided to the application writer's computer. As acknowledged by the Examiner, no unique owner's key is assigned to the destination computer or even hinted at and, therefore, cannot be used to compute a first signature, comprising a selected hash value encrypted by the owner's key, and appended to the software file. The user is presumed to have a secure processing device that can hash the received software file to produce a first hash value. The Chang Patent, as acknowledged by the Examiner, does not assign a unique owner's key to the destination computer and, therefore, cannot encrypt the first hash value with the owner's key to generate a second signature. Therefore, there is no first signature, comprising a selected hash value encrypted by the owner's key, or second signature, comprising the result of encrypting the first hash value with the owner's key.	The Ho Patent is limited to a self-contained storage medium and a network interface card. The Ho Patent does not even hint at the use of a unique owner's key that is assigned to the destination computer and, therefore, a unique owner's key that is assigned to the destination computer cannot be used to compute a first signature, comprising a selected hash value encrypted by the owner's key, and appended to the software file. The user is presumed to have a secure processing device that can hash the received software file to produce a first hash value. The Ho Patent does not assign a unique owner's key to the destination computer and, therefore, cannot encrypt the first hash value with the owner's key to generate a second signature. Therefore, there is no first signature, comprising a selected hash value encrypted by the owner's key, or second signature, comprising the result of encrypting the first hash value with the owner's key.

VII. Lack of Motivation or Suggestion to Combine References

In order to meet the first of the above-noted three requirements by the MPEP for prima facie obviousness, the following must be shown: 1.) one or more references; 2.) the references were available to the inventor at the time of the claimed invention; 3.) each of the references teaches an element of the claimed invention; 4.) the prior art contains a suggestion or a motivation to combine the references; and 5.) the combination of the references would have made the invention obvious. See *In re Rinehart*, 189 USPQ 143, 147 (C. C. P. A. 1976); *In re Fine*, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988); *In re Fitch*, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992).

Discussion of the deficiencies in these five factors in the Examiner's rejection:

In reference to factors 1. – 3., the Examiner has cited and relied on the knowledge of those skilled in the art of file encryption technology as a basis for his rejection of claims 1 – 15 and 18 under 35 U.S.C. §103(a). Neither the cited Chang Patent, nor the cited Ho Patent Application Publication, nor the cited Horstmann Patent discloses a unique owner's key that is assigned to the destination computer. Since there is no owner's key, neither the cited Chang Patent, nor the cited Ho Patent Application Publication, nor the cited Horstmann Patent discloses a system that computes a first signature, comprising a selected hash value encrypted by the owner's key, and appended to the software file. Since there is no owner's key, neither the cited Chang Patent, nor the cited Ho Patent Application Publication, nor the cited Horstmann Patent discloses a system that encrypts the first hash value with the owner's key to generate a second signature. Since there is no owner's key, neither the cited Chang Patent, nor the cited Ho Patent Application Publication, nor the cited Horstmann Patent discloses a system that generates a second signature, comprising the result of encrypting the first hash value with the owner's key.

Thus, the Examiner provides no indication in the cited references that would provide a motivation or suggestion for combining the teachings of the cited Chang Patent and the cited Ho Patent Application Publication and the cited Horstmann Patent or any teachings contained in these references that would render Appellants' claimed invention obvious. An essential evidentiary showing by the Examiner of a suggestion or motivation to combine the prior references relied upon in a manner that would render the claimed invention obvious has not been made. *In re Rouffet*, 47

U.S.P.Q. 2d 1453 (Fed. Cir. 1998); *C.R. Bard, Inc. v. M3 Systems, Inc.*, 48 U.S.P.Q. 2d 1225 (Fed. Cir. 1998).

With respect to MPEP Requirements 4. and 5. noted above, the courts and the MPEP have stated that a motivation to combine references must be found in the prior art. See MPEP 2143.01:

> Obviousness cannot be established by combining teachings of the prior art to produce the claimed invention absent some teaching suggesting or incentive supporting the combination. *In re Geiger*, 2 USPQ2d 1276, 1278 (Fed. Cir. 1987)

The courts have further stated that the motivation or combination must be shown in the prior art:

> In order to combine references, there must be some suggestion or motivation for doing so in the prior art either in the references themselves or elsewhere. *In re Jones*, 21 USPQ2d 1941, 1942 (Fed. Cir. 1992)

The courts have further stated:

> The mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggests the desirability of the modification. *In re Fritch*, 23 USPQ2d 1780, 1783-1784 (Fed. Cir. 1992).

The Examiner states a belief that it would be obvious to combine the teachings of the three cited references in a piecemeal manner, but fails to indicate any suggestion contained within the references themselves or elsewhere that would support this conclusion, and overlooks the specific teaching away from Appellants' claimed invention by the cited Chang U.S. Patent and the cited Ho U.S. Published Patent Application and the cited Horstmann U.S. Patent, as noted above. If any combination of the cited Chang U.S. Patent and the cited Ho U.S. Published Patent Application and the cited Horstmann U.S. Patent was proper (and it is not), it would still not result in the Appellants' claimed invention.

VIII. Summary

Appellants believe that claims 1 – 15 and 18 are allowable under 35 U.S.C. §103(a) over the cited Chang U.S. Patent and the cited Ho U.S. Published

Patent Application and the cited Horstmann U.S. Patent for the reasons articulated above.

Appellants respectfully request a Notice of Allowance in this application in light of the arguments set forth herein. The undersigned attorney requests Examiner Szymanski to telephone if a conversation could expedite the prosecution of this application. Appellants authorize the Commissioner to charge any additionally required payment of fees to our Deposit Account No. 50-1848, under Order No. 013217.0177PTUS from which the undersigned is authorized to draw.

Respectfully submitted,
PATTON BOGGS LLP

Dated: 21 AUGUST 2006

By: _____
James M. Graziano
Registration No.: 28,300
(303) 830-1776
(303) 894-9239 (Fax)
Attorney for Applicants

Customer No. 24283

8. CLAIMS APPENDIX

1. (Previously presented) A secure data authentication apparatus to authenticate a software file, the software file having a first signature appended to the software file, for use on a computer system, wherein said computer system is assigned an owner key that is unique to said computer system, said first signature comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said owner key to produce said first signature, the apparatus comprising:

a secure processing device within the computer system to receive the software file and hash the software file using said selected hash function to produce a first hash value; and

a first key located within the secure processing device, which first key comprises said owner key wherein the secure processing device encrypts the first hash value with the first key to generate a second signature and compares the first signature with the second signature, and if the first signature matches the second signature, the computer system accepts the software file as being authenticated.

2. (Previously presented) The secure data authentication apparatus of claim 1 wherein the software file further comprises a first source signature appended to the software file, the apparatus further comprising:

a source key located within the secure processing device, wherein the secure processing device encrypts the first hash value with the source key to generate a second source signature and compares the first source signature with the second source signature, and if the first source signature matches the second source signature, the computer system accepts the software file as being authenticated from the source represented by the first source signature.

3. (Previously presented) The secure data authentication apparatus of claim 1 wherein the software file further comprises a first owner signature appended to the software file, the apparatus further comprising:

an owner key located within the secure processing device, wherein the secure processing device encrypts the first hash value with the owner key to generate a

second owner signature and compares the first owner signature with the second owner signature, and if the first owner signature matches the second owner signature, the computer system accepts the software file as being authenticated.

4. (Previously presented) The secure data authentication apparatus of claim 1, further comprising:

a key exchange request having a first key exchange signature appended thereto, the key exchange request sent from the computer system to the secure processing device, wherein the secure processing device hashes the key exchange request to generate a second hash value;

a first key exchange key located within the secure processing device, wherein the secure processing device encrypts the second hash value with the first key exchange key to generate a second key exchange signature and compares the first key exchange signature with the second key exchange signature, and if the first key exchange signature matches the second key exchange signature, the secure processing device erases the first owner key; and

a second owner key within the key exchange request, wherein the secure processing device saves the second owner key.

5. (Previously presented) The secure data authentication apparatus of claim 4 wherein the computer system further comprises a first feature file and the computer system performs in accordance with the first feature file, the apparatus further comprising:

a second feature file having a third owner signature appended thereto, wherein the secure processing device hashes the second feature file to generate a third hash value which is encrypted with the second owner key to generate a fourth owner signature and compares the third owner signature with the fourth owner signature, and if the third owner signature matches the fourth owner signature, the computer system replaces the first feature file with the second feature file.

6. (Previously presented) The secure data authentication apparatus of claim 1 wherein the program comprises a feature file having a plurality of features

wherein a subset of the plurality of features are activated and the computer system operates in accordance with the subset of the plurality of features.

7. (Previously presented) A secure data authentication apparatus to authenticate an owner of a software file and of a telephony switching system on which the software file is stored, the apparatus comprising:

a first feature file and a software file, the first feature file having a plurality of features and a first owner signature appended thereto, wherein said telephony switching system is assigned a first owner key that is unique to said telephony switching system, said first owner signature comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said first owner key to produce said first owner signature, wherein a first subset of the plurality of features is activated;

a secure microprocessor within the telephony switching system, the secure microprocessor having an encryption algorithm, wherein the secure microprocessor hashes the first feature file using said selected hash function to generate a first hash value; and

a first owner key within the secure microprocessor, wherein the secure microprocessor encrypts the first hash value with the first owner key to generate a second owner signature and the secure microprocessor compares the first owner signature with the second owner signature, and if the first owner signature matches the second owner signature, the telephony switching system operates in accordance with the first subset of the plurality of features of the first feature file.

8. (Previously presented) The secure data authentication apparatus of claim 7, the apparatus further authenticating a source of the software file, the apparatus further comprising:

a first source signature appended to the first feature file; and

a source key located within the secure microprocessor, wherein the secure microprocessor encrypts the first hash value with the source key to generate a second source signature and the secure microprocessor compares the first source signature with the second source signature, and if the first source signature matches the second

source signature, the telephony switching system operates in accordance with the first subset of the plurality of features of the first feature file.

9. (Previously presented) The secure data authentication apparatus of claim 7, further comprising:

a second feature file having a second subset of the plurality of features activated, the second feature file having a third owner signature appended thereto; wherein the secure microprocessor receives the second feature file and hashes the second feature file to generate a second hash value and encrypts the second hash value with the first owner key to generate a fourth owner signature, and the secure microprocessor compares the third owner signature with the fourth owner signature, and if the third owner signature matches the fourth owner signature, the second feature file is written over the first feature file.

10. (Previously presented) A method for authenticating an owner of a software file that has a first identification code comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using an owner key to produce said first signature, attached thereto for use on a computer system, wherein said computer system is assigned said owner key that is unique to said computer system, the computer system comprising a secure processor having an encryption algorithm and an owner key, the method comprising:

initiating the computer system;

hashing the software file using said selected hash function within the secure processor to generate a first hash value;

encrypting the first hash value with the owner key to generate a second identification code; and

comparing the first identification code with the second identification code, and if the first identification code matches the second identification code, the computer system accepts the software file as being authenticated for the owner's use.

11. (Previously presented) A method for authenticating an owner of a software file that has a first owner signature comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using an owner key to produce said first signature, appended to the software file, for use on a computer system, wherein said computer system is assigned said owner key that is unique to said computer system, having a secure processing device to generate an authorization signal, the secure processing device comprising a security routine, an encryption algorithm and a first owner key, the process comprising:

receiving the software file by the computer system and sending the software file to the secure processing device;

hashing the software file using said selected hash function to generate a first hash value;

encrypting the first hash value within the secure processing device with the first owner key to generate a second owner signature; and

comparing the first owner signature to the second owner signature, wherein if the first owner signature and the second owner signature match, the secure processing device generates the authorization signal.

12. (Previously presented) The method for authenticating an owner of the software file of claim 11 wherein the software file further comprises a first source signature appended thereto and the secure processing device further comprising a source key; the method further authenticating a source of the software file, the method comprising:

encrypting the first hash value within the secure processing device with the source key to generate a second source signature; and

comparing the first source signature to the second source signature, wherein if the first source signature and the second source signature match, the secure processing device generates the authorization signal.

13. (Previously presented) The method for authenticating an owner of the software file of claim 11 wherein the secure processing device further comprises a first key exchange key, the method further comprising:

receiving a key exchange request by the secure processing device, the key exchange request including an encrypted second owner key and having a first key exchange signature appended thereto;

hashing the key exchange request to generate a second hash value;

encrypting the second hash value with the first key exchange key to generate a second key exchange signature; and

comparing the first key exchange signature with the second key exchange signature, wherein if the first key exchange signature and the second key exchange signature match, the secure processing device decrypts the second owner key and replaces the first owner key with the decrypted second owner key.

14. (Previously presented) The method for authenticating an owner of a software file of claim 13 wherein the key exchange request further comprises an encrypted second key exchange key, the authenticating method further comprising:

decrypting the encrypted second key exchange key with the first key exchange key; and

replacing the first key exchange key located within the secure processing device with the decrypted second key exchange key.

15. (Previously presented) The method for authenticating a source and an owner of a software file of claim 13 wherein the computer system further comprises a first feature file having a first plurality of features, wherein a first subset of the first plurality of features is activated and the computer system performs in accordance with the first subset of the first plurality of features, the method further comprising:

receiving a second feature file having a third owner signature appended thereto, the second feature file comprising a second plurality of features wherein a second subset of the second plurality of features is activated;

hashing the second feature file within the secure processing device to generate a third hash value;

encrypting the third hashed file with the second decrypted owner key within the secure processing device to generate a fourth owner signature; and

comparing the third owner signature with the fourth owner signature, wherein if the third owner signature matches the fourth owner signature, the computer system overwrites the first feature file with the second feature file, and the computer system performs in accordance with the second subset of the second plurality of features.

Claims 16 and 17 (Canceled)

18. (Previously presented) A method for authenticating a software file from a PBX manufacturer, the software file comprising a feature file having a plurality of features wherein a subset of the plurality of features are activated, the software file operating on a PBX, the PBX comprising a secure microprocessor having an encryption algorithm and a first key that is unique to said PBX, the method comprising:

hashing the feature file using a selected hash function at the PBX manufacturer to generate a first hash value;

encrypting the first hash value with said first key to generate a first signature;

appending the first signature to the feature file;

receiving the feature file and appended first signature by the secure microprocessor;

hashing the received feature file using said selected hash function within the secure microprocessor to generate a second hash value;

encrypting the second hash value with the first key to generate a second signature; and

comparing the first signature with the second signature, and if the first signature matches the second signature, the PBX accepts the software file as being authenticated.

9.) EVIDENCE APPENDIX

None

10.) RELATED PROCEEDINGS APPENDIX

None